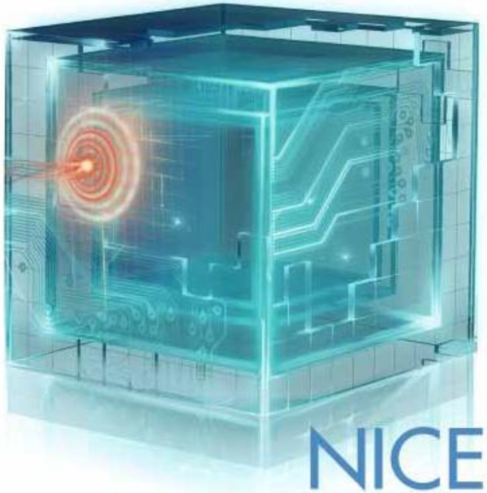
THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

INTERACTIVE HOW-TO AND IMPLEMENTATION GUIDE



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Cybersecurity is a National Concern

Your help is critical to defining the Nation's cybersecurity workforce!

Effective cybersecurity management is essential to protecting our nation's technology infrastructure. The professionals accountable for this protection constitute a critical workforce. Until now, there has been little consistency in terms of how cybersecurity work is defined and categorized, who is responsible for the work, and what skill sets are needed to perform successfully. Even within organizations, individuals performing cybersecurity work are difficult to identify, locate, and quantify. As a nation, we must establish consistency in how the cybersecurity workforce is defined and classified.

With the direct engagement of over 20 Federal departments and agencies, and numerous public and private organizations, the National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework (the Framework) to define cybersecurity work and lay a foundation for cybersecurity workforce efforts. The Framework provides a common language and taxonomy and defines specialty areas, knowledge, skills, and abilities (KSAs), and codifies talent.

This how-to guide explains what the Framework is, and why you need to not only be aware of the Framework, but also adopt it according to your organization's needs. Explore the guide using the Navigation Bar and by clicking on other links.

Along with representatives from departments and agencies listed on the right, I would like to be among the first to thank you for your support.

Ernest McDuffie

Ernest McDuffie, National Institute for Standards & Technology

The following organizations participated in the development of the Framework, among others:

- Department of State
- Department of Education
- Department of Labor
- Office of Management and Budget
- Office of Personnel Management
- Department of Defense
- Department of Justice
- Information Sciences & Technologies
- Department of Homeland Security
- Central Intelligence Agency
- Defense Intelligence Agency
- Director of National Intelligence
- Federal Bureau of Investigation
- National Security Agency
- National Science Foundation
- Department of Defense National Counterintelligence Executive
- Federal Chief Information Officers Council

"As a nation, we must establish consistency in how the cybersecurity workforce is defined and classified."

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

This Guide Answers Your Questions

→ What is the National Cybersecurity Workforce Framework? How was it developed?

→ What are the 7 categories of cybersecurity work?

→ What are the 31 cybersecurity specialty areas?

→ What are the benefits to adopting the Framework?

→ How does the Framework impact the Human Capital Management (HCM) Lifecycle?

→ How do I help my organization adopt the Framework?

→ How can I use the Framework to define my organization's cybersecurity roles?

→ Are there any sample roles my organization can easily and quickly adopt?

→ My organization has many cybersecurity positions.
Can I develop customized cybersecurity roles?

→ How does the Framework support competency model development?
Can I see an example?

→ How does the Framework support workforce analytics?
Can I see an example?

→ What's next in terms of cybersecurity workforce development?
What other products can I see soon?

This is an interactive guide created to provide you with information about adopting the National Cybersecurity Workforce Framework. The links on the left, and other important links on each page, help you navigate the guide. If, at any time, you would like to return to this page, click on "Contents."

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

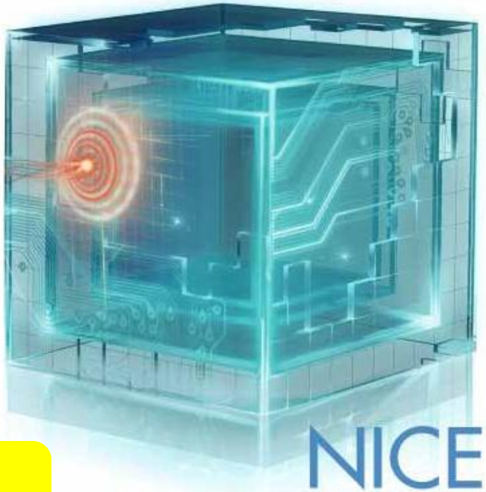
What is the Framework?

The National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework (the Framework) to define the cybersecurity workforce and provide a common taxonomy and lexicon by which to classify and categorize workers.

- **The Framework is a dictionary.** Defining the cybersecurity population consistently, and using standardized terms, is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. The Framework lists and defines 31 specialty areas of cybersecurity work and provides a description of each. Each of the types of work is placed into 1 of 7 overall categories. The Framework also identifies common tasks and knowledge, skills, and abilities (KSAs) associated with each specialty area.

- **The Framework is a tool.** It provides the groundwork, or a baseline, by which organizations can develop their Human Capital Management programs, including defining roles, designing competency models, standardizing job descriptions, and providing specialized training. The Framework will be used as guidance to the federal government, will be made available to the private, public, and academic sectors for describing cybersecurity work and workforces, and related education, training, and professional development.

- **The Framework is a collaboration.** The Framework was developed as a direct result from the White House's need to quickly identify, quantify, and develop an effective cybersecurity workforce to develop our Nation's critical cyber infrastructure. The Framework is the output of a collaboration of over 20 Federal departments and agencies and numerous national organizations from within academia and general industry. Each recognized a need to define the Nation's cybersecurity workforce. After an extensive review process, the Framework was finalized and approved by the Office of Management and Budget in September 2012.



Click HERE to see a sample page from the Framework.
And click HERE to visit a full version of the Framework online.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

[Contents](#)

[What is the Framework?](#)

[Categories](#)

[Specialty Areas](#)

[Benefits](#)

[HCM Impact](#)

[Adoption](#)

[STEP 1: Role Definition](#)

- [Streamlined Roles](#)
- [Customized Roles](#)

[STEP 2: Model Competencies](#)

[STEP 3: Plan Your Workforce](#)

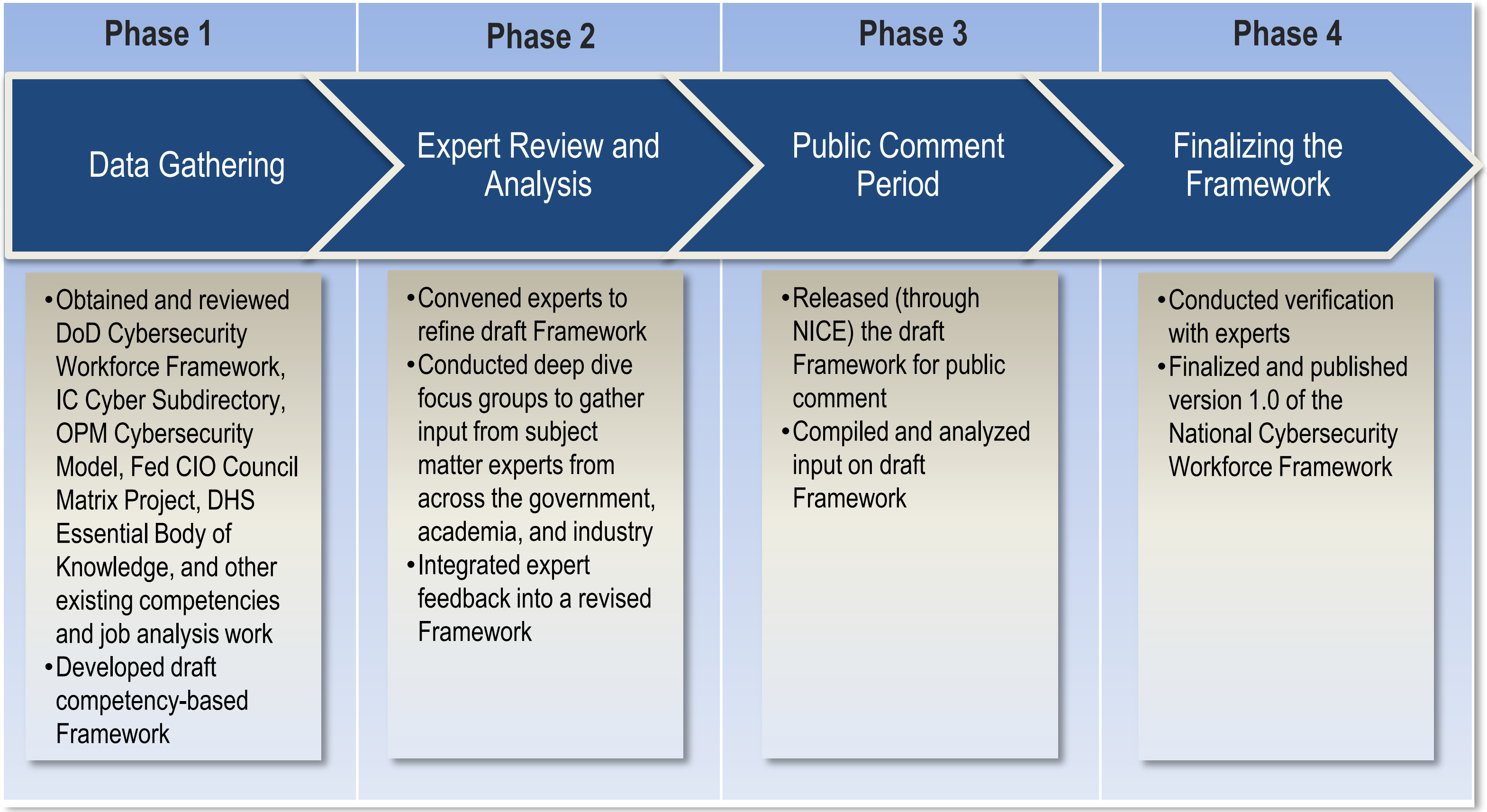
[STEP 4: Plan for the Future](#)

[Contact Us](#)

How was the Framework Developed?

The Framework was developed consistent with professional guidelines and best practices. Using a comprehensive job analytic approach, data was collected from across the government, and additional information was gathered from academia and the public and private sectors.

The Framework was developed according to the following steps:



Phase 1

Data Gathering

- Obtained and reviewed DoD Cybersecurity Workforce Framework, IC Cyber Subdirectory, OPM Cybersecurity Model, Fed CIO Council Matrix Project, DHS Essential Body of Knowledge, and other existing competencies and job analysis work
- Developed draft competency-based Framework

Phase 2

Expert Review and Analysis

- Convened experts to refine draft Framework
- Conducted deep dive focus groups to gather input from subject matter experts from across the government, academia, and industry
- Integrated expert feedback into a revised Framework

Phase 3

Public Comment Period

- Released (through NICE) the draft Framework for public comment
- Compiled and analyzed input on draft Framework

Phase 4

Finalizing the Framework

- Conducted verification with experts
- Finalized and published version 1.0 of the National Cybersecurity Workforce Framework

[Click HERE to see a sample page from the Framework.](#)

[And click HERE to visit a full version of the Framework online.](#)

What are the 7 Categories?

The Framework establishes a common taxonomy and lexicon for cybersecurity workers. The 7 categories, serving as an overarching structure for the Framework, group related specialty areas together.

The categories of cybersecurity work, and their definitions, are in the table below.

Securely Provision	Specialty areas concerned with conceptualizing, designing, and building secure IT systems.
Operate and Maintain	Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
Protect and Defend	Specialty areas responsible for identifying, analyzing, and mitigating threats to IT systems.
Investigate	Specialty areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
Collect and Operate	Specialty areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
Analyze	Specialty area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
Oversight and Development	Specialty areas that provide critical support so others may conduct their cybersecurity work.

Click HERE to see a sample page from the Framework.

And click HERE to visit a full version of the Framework online.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

What are the 31 Specialty Areas?

Each specialty area represents an area of concentrated work, or function, within cybersecurity. The Framework provides the typical tasks and knowledge, skills and abilities (KSAs) within each specialty area.

Securely Provision

Systems Requirements Planning
Systems Development
Software Assurance and Security Engineering
Systems Security Architecture
Test and Evaluation
Technology Research and Development
Information Assurance (IA) Compliance

Operate and Maintain

System Administration
Network Services
Systems Security Analysis
Customer Service and Technical Support
Data Administration
Knowledge Management

Collect and Operate

Collection Operations
Cyber Operations Planning
Cyber Operations

Protect and Defend

Vulnerability Assessment and Management
Incident Response
Computer Network Defense (CND) Analysis
Computer Network Defense (CND) Infrastructure Support

Investigate

Investigation
Digital Forensics

Analyze

Threat Analysis
Exploitation Analysis
Targets
All Source Intelligence

Oversight and Development

Legal Advice and Advocacy
Education and Training
Strategic Planning and Policy Development
Information Systems Security Operations (ISSO)
Security Program Management (Chief Information Security Officer [CISO])

Click HERE to see a sample page from the Framework.
And click HERE to visit a full version of the Framework online.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

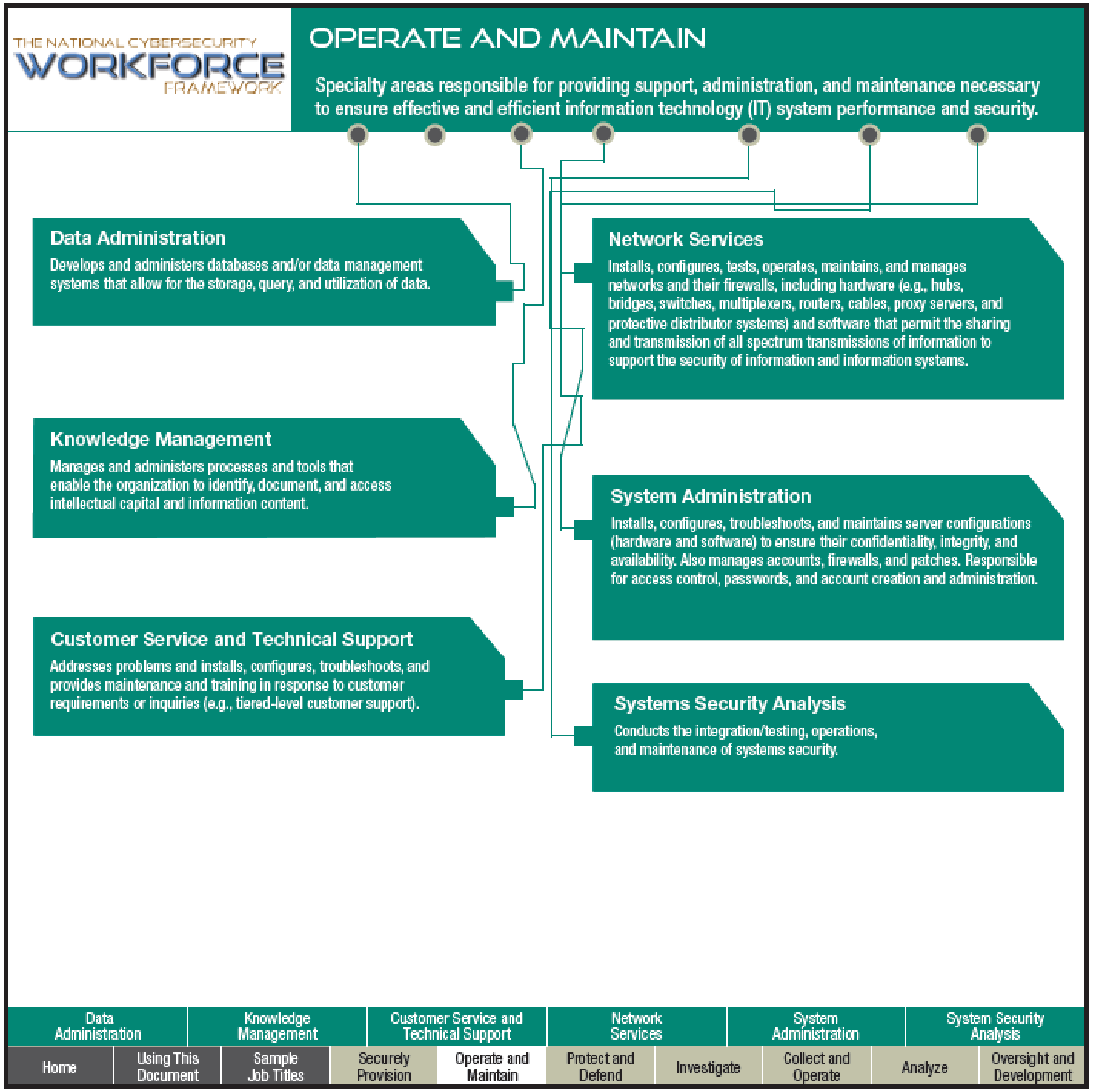
Sample Page from the Framework

This is a sample page from the Framework.

This is the "Operate and Maintain" cybersecurity functional category.

Within this category, there are 7 specialty areas, including:

- Data Administration
- Network Services
- Knowledge Management
- System Administration
- Customer Service and Technical Support
- Systems Security Analysis



THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

OPERATE AND MAINTAIN

Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

Data Administration
Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

Network Services
Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

Knowledge Management
Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

System Administration
Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

Customer Service and Technical Support
Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

Systems Security Analysis
Conducts the integration/testing, operations, and maintenance of systems security.

Click HERE to visit a full version of the Framework online.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

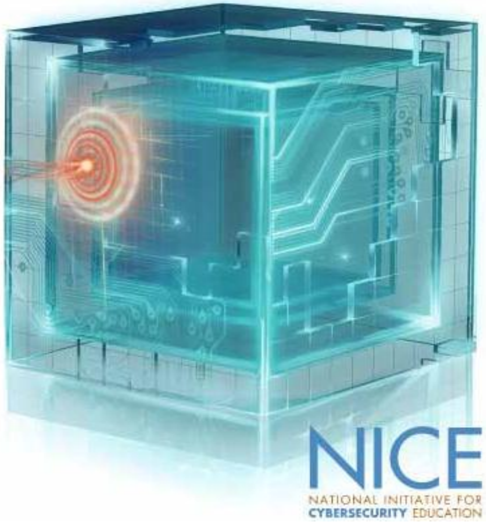
STEP 4: Plan for the Future

Contact Us

What are the Benefits of The Framework?

The Framework benefits organizations, the workforce, and even the Nation, by defining cybersecurity functions and creating a common taxonomy which can be used when referring to cybersecurity work. The purpose of the Framework is to describe cybersecurity work irrespective of organizational structures, job titles, or other potentially individual conventions. The Framework does the following:

- ✓ Provides consistent language, and a working taxonomy, organizations can use to describe and define their cyber workforces. It supports skill assessment and gap identification that can identify the training needed to develop and maintain a high-performing, diverse workforce.
- ✓ Aids in the classification of workers into common cyber roles, which helps streamline human capital efforts.
- ✓ Assists organizations to better meet workload needs, including adjusting their recruitment and selection procedures to focus on applicants with specific skills sets, developing or choose training programs that align with the KSAs identified within the Framework, and planning for future workforce needs.
- ✓ Helps organizations respond to mandates and surveys. The Office of Personnel Management (OPM) is implementing a data element which will be coded to every cybersecurity worker, and the Federal Network Security Management Act (FISMA) data collection survey will require input on the extent of each Federal agency's adoption of the Framework.
- ✓ Overall, creates consistent role definitions, and promotes understanding, of the type of work required of cybersecurity professionals.



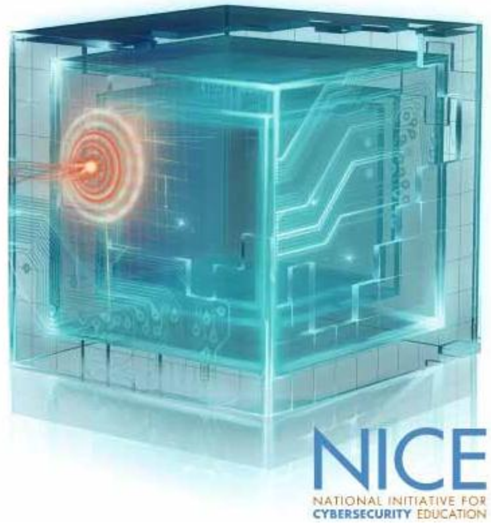
How do I use the OPM Data Element?

OPM has developed data standards, or data elements, to facilitate the use of Federal civilian human resources data. The standards also help avoid unnecessary duplication and incompatibility in the collection, process, and dissemination of such data.

OPM will require agencies to utilize cybersecurity codes specifically developed to identify these positions across occupational series in the Enterprise Human Resources Integration (EHRI) status and dynamic submissions. The usual timeframe allowed to service providers varies from 9 – 18 months to reprogram their systems. Once the programming is completed, and agencies are able to submit data in EHRI, then reports can be requested from the OPM Data Analysis group. The data element standards satisfy information needs, are maintained by human resources professionals, and coordinated by the Office of the Chief Information Officer.

The OPM Data element will:

- ✓ Identify positions for which the primary function is cybersecurity.
- ✓ Enable OPM and Federal agencies to identify the cybersecurity workforce, determine baseline capabilities, examine hiring trends, identify skill gaps, and more effectively recruit, hire, train, develop and retain an effective cybersecurity workforce.
- ✓ Allow HR Professionals to better understand their workforce and what issues need to be addressed.
- ✓ Provide a similar platform for organizations outside of the Federal Government to organize their cybersecurity professionals.



Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

What is the OPM Data Element?

The OPM Data Elements are derived directly from the Framework's Categories and Specialty Areas (http://csrc.nist.gov/nice/framework/). Selection of a Data Element (or a Cybersecurity Category or Specialty Area) should be based upon the duties in which the incumbent is primarily engaged or which best reflects the requirements of the job.

The OPM cybersecurity data standards, or data elements, were published on October 1, 2012. A link to the **OPM's Guide to Data Standard**, where the Data Element is published, is here.

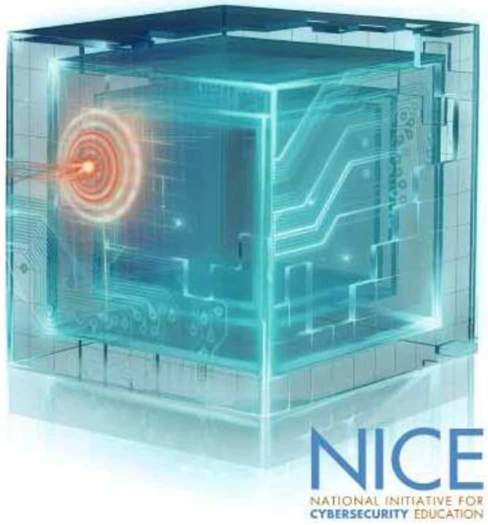
In February 2012, the President issued the Cross Agency Priority (CAP) goal to close critical skill gaps in the Federal workforce to improve mission performance. In September, OPM designated IT-Cybersecurity as one of three priority occupations for closing skills gaps. The Cybersecurity Data Element was developed by OPM to facilitate agency strategic workforce planning to achieve the goal to close critical Federal skill gaps. (This reinforces the need to clearly identify these positions throughout the government.)

Key points to using the OPM Data Element include:

✓ Only one code is permitted so it is important that the most appropriate code is used and that the codes are used consistently.

✓ If the work of an incumbent or the requirements of a position are predominantly in one Specialty Area, that code should be used.

✓ If there are multiple relevant Specialty Areas within a Category and no single Specialty Area predominated, the code for the Category in which those Specialty Areas fall should be used.



Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

OPM Data Elements

The OPM Cybersecurity Data Elements are in the tables on the following pages.

Code	Category/Specialty Area Label and Definition
00	**Not Applicable** - Position does not involve work in one or more cybersecurity functions.
10	**Analyze** - Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
11	**All Source Intelligence** - Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places information in context; draws insights about the possible implications.
12	**Exploitation Analysis** - Analyzes collected information to identify vulnerabilities and potential for exploitation.
13	**Targets** - Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.
14	**Threat Analysis** - Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.
20	**Investigate** - Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.
21	**Digital Forensics** - Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.
22	**Investigation** - Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.
30	**Collect and Operate** - Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
31	**Collection Operations** - Executes collection using appropriate strategies and within the priorities established through the collection management process.
32	**Cyber Operations** - Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

OPM Data Elements (continued)

Code	Category/Specialty Area Label and Definition
33	**Cyber Operations Planning** - Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.
40	**Operate and Maintain** - Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
41	**Customer Service and Technical Support** - Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).
42	**Data Administration** - Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.
43	**Knowledge Management** - Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.
44	**Network Services** - Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
45	**System Administration** - Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.
46	**Systems Security Analysis** - Conducts the integration/testing, operations, and maintenance of systems security.
50	**Protect and Defend** - Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.
51	**Computer Network Defense (CND) Analysis** - Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.
52	**Computer Network Defense (CND) Infrastructure Support** - Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

OPM Data Elements (continued)

Code	Category/Specialty Area Label and Definition
53	**Incident Response** - Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
54	**Vulnerability Assessment and Management** - Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.
60	**Securely Provision** - Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).
61	**Information Assurance (IA) Compliance** - Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
62	**Software Assurance and Security Engineering** - Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.
63	**Systems Development** - Works on the development phases of the systems development lifecycle.
64	**Systems Requirements Planning** - Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
65	**Systems Security Architecture** - Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
66	**Technology Research and Development** - Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
67	**Test and Evaluation** - Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of elements of systems incorporating IT.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

OPM Data Elements (continued)

Code	Category/Specialty Area Label and Definition
70	**Oversight and Development** - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.
71	**Education and Training** - Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.
72	**Information Systems Security Operations (Information Systems Security Officer [ISSO])** - Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.
73	**Legal Advice and Advocacy** - Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
74	**Security Program Management (Chief Information Security Officer [CISO])** - Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.
75	**Strategic Planning and Policy Development** - Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.
80	**Cybersecurity Program/Project Management** - Manages one or more cybersecurity project(s) or program(s) to provide products and/or services. Coordinates, communicates and integrates cybersecurity projects and program activities. Ensures cybersecurity work efforts achieve the intended or specified outcomes. May encompass the decision-making and negotiation responsibilities involved in executing the program efforts.
90	**Cybersecurity Supervision, Management, and Leadership** - Supervises, manages, and/or leads work and workers performing cybersecurity work (i.e., the work described in the Categories and Specialty Area codes with values 10-75). Given that the supervisor oversees individuals with a range of specialty areas, this can encompass multiple various specialty areas.

[Contents](#)

[What is the Framework?](#)

[Categories](#)

[Specialty Areas](#)

[Benefits](#)

[HCM Impact](#)

[Adoption](#)

[STEP 1: Role Definition](#)

- [Streamlined Roles](#)
- [Customized Roles](#)

[STEP 2: Model Competencies](#)

[STEP 3: Plan Your Workforce](#)

[STEP 4: Plan for the Future](#)

[Contact Us](#)

Assigning the Data Element (Examples)

Below are examples of how position descriptions can be analyzed and linked to an OPM Cybersecurity Data Element. When assigning a code, it is critical for HR representatives, supervisors, and hiring managers to work in a collaborative effort to best determine which code should be used.

Example 1: An employee's duties fall within the work expected of one Specialty Area.

- Job Description Excerpt: "…the employee works on the development of the systems' lifecycle..."
- Data Element: **Code 63, Systems Development**.

Example 2: An employee's duties fall within multiple Specialty Areas in one Category.

- Job Description Excerpt: "…responsible for identification and mitigation of threats to internal information technology (IT) systems or networks, uses defensive measures collected from a variety of sources to identify, analyze, and report events that occur, monitors network to actively remediate unauthorized activities and responds to crisis or urgent situations to mitigate immediate and potential threats..."
- Data Element: **Code 50, Protect and Defend Category**. The category is used since work refers to multiple specialty areas.

Example 3: A manager oversees workers with duties in one Specialty Area.

- Job Description Excerpt: "…oversees workers who develop and write/code new computer applications, software, or specialized utility programs following software assurance best practices..."
- Data Element: **Code 62, Software Assurance and Security Engineering**.

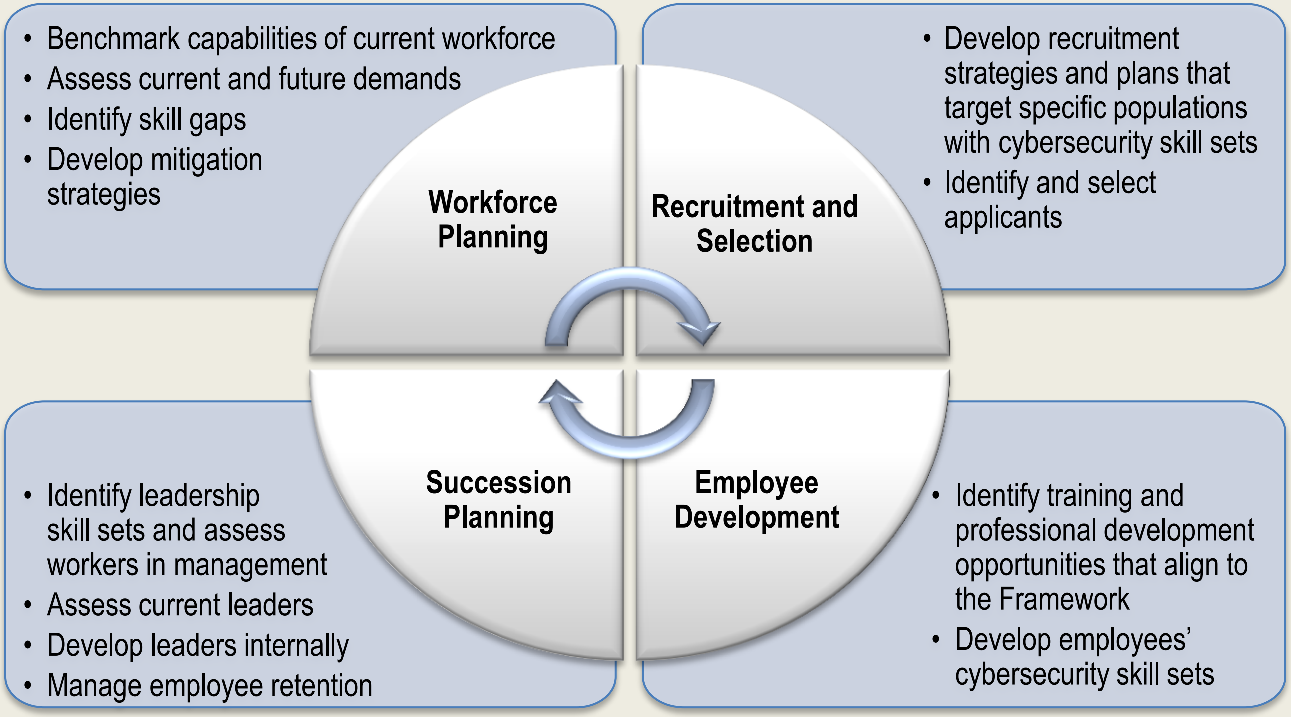
Example 4: A manager oversees workers with duties in multiple Specialty Areas/Categories.

- Job Description Excerpt: "…manages individuals that process tools enabling the organization to identify, document, and access intellectual capital and information content, applies current knowledge of one or more regions, countries, non-state entities, and/or technologies, and supervises, manages, and/or leads work and workers performing cybersecurity work…"
- Data Element: **Code 90, Cybersecurity Supervision, Management and Leadership**. This code is selected because the position is a supervisory one that monitors employees whose work spans over multiple specialty areas (codes 13 and 43).

How is Human Capital Management Impacted?

The Framework enhances understanding of cybersecurity work and creates consistency. The Framework impacts every aspect of the Human Capital Management (HCM) Lifecycle.

Human Capital Management (HCM) Lifecycle



Workforce Planning:

- Benchmark capabilities of current workforce
- Assess current and future demands
- Identify skill gaps
- Develop mitigation strategies

Recruitment and Selection:

- Develop recruitment strategies and plans that target specific populations with cybersecurity skill sets
- Identify and select applicants

Succession Planning:

- Identify leadership skill sets and assess workers in management
- Assess current leaders
- Develop leaders internally
- Manage employee retention

Employee Development:

- Identify training and professional development opportunities that align to the Framework
- Develop employees’ cybersecurity skill sets

For your organization to effectively manage its HCM lifecycle for cybersecurity, it is recommended you take these steps:

- ➢ STEP 1: Define your organization’s cybersecurity roles according to the Framework
- ➢ STEP 2: Develop competency models for your cybersecurity workers
- ➢ STEP 3: Conduct workforce planning to establish your cybersecurity needs
- ➢ STEP 4: Plan for the future (recruit, select, develop, succession planning)

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

How can you Adopt the Framework?

The Framework's taxonomy can be overlaid onto an existing organizational structure to provide standardization of common cybersecurity tasks, specialty areas, KSAs, and recommended job titles. The Framework can be customized for specific organization components or generalized across entire organizations. Since the size and scope of cybersecurity workforces vary by organization, different methods of adopting the Framework can be applied.

Here is a recommended process that can help your organization adopt the Framework.

STEP 1

Define Cybersecurity Roles

Assess your cybersecurity workforce and ensure your roles are consistent with the Framework. Click HERE to see an example process that can help guide your work. These are the cybersecurity roles developed by the Federal Chief Information Officers Council (Fed CIOC), which you can use within your own organization.

STEP 2

Develop Cybersecurity Competency Models

Once you define your organization's Framework-based cybersecurity roles, you can then develop competency models for these individuals. (Federal guidance requires every department and agency to develop competency models for workers.) Click HERE for an example of how this is being done by DHS's Cybersecurity Workforce Initiative.

STEP 3

Conduct Workforce Planning

Use your newly defined cybersecurity roles to gather and assess data that can be used for future workforce planning efforts. Click HERE to see an example of the methodology you can use.

STEP 4

Plan for the Future

Once those activities are accomplished, and based on the gaps found after completing workforce planning, you can develop strategies for other Human Capital efforts within your organization, such as recruitment, selection, succession planning, and employee development.

STEP 1: Role Definition

The first step of adopting the Framework is to define and list your organization's cybersecurity roles.

You can adopt a set of generalized roles by using the streamlined application developed by the Federal Chief Information Officers Council (Fed CIOC), or you can develop your own cybersecurity roles by using the custom application illustrated by the Department of Homeland Security (DHS).

Streamlined Application

- Recommended for organizations with limited resources (such as personnel to dedicate to this task), or those with typical cybersecurity duties.
- The streamlined application defines general cybersecurity roles by combining Framework specialty areas into broader areas of responsibility.
- The Fed CIOC developed 13 roles to demonstrate this application. Those roles are in this guide.

Custom Application

- Recommended for organizations with more resources, or those with many unique or specialized cybersecurity roles.
- Defines and characterizes specialized cybersecurity roles and identifies competencies.
- Demonstrated by DHS's Cybersecurity Workforce Initiative (CWI).

Click HERE for the process of choosing and applying a role application.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

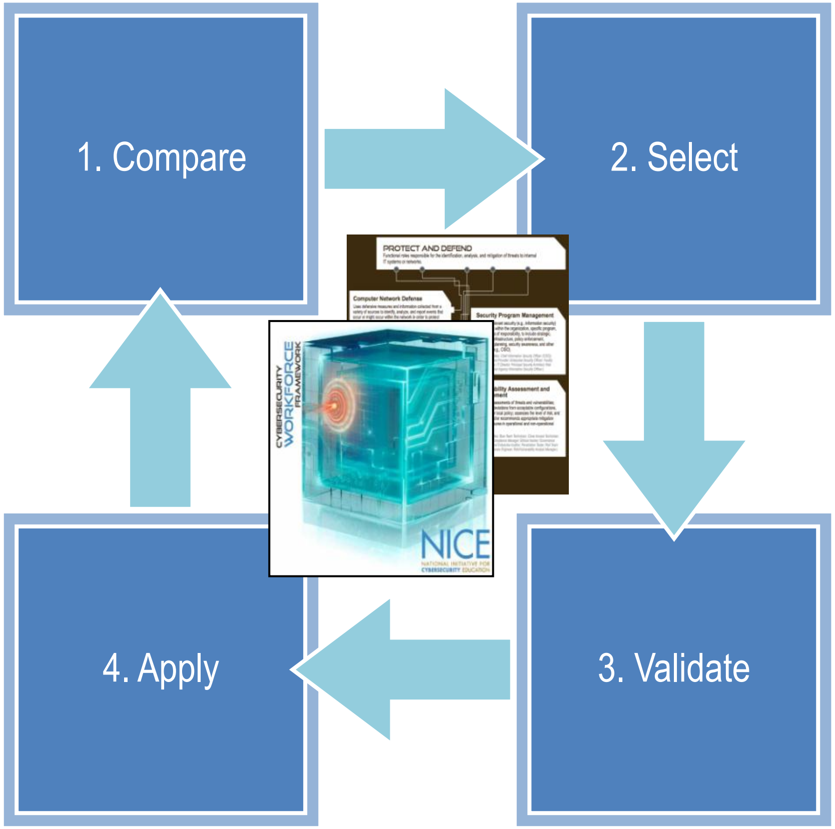
STEP 4: Plan for the Future

Contact Us

Role Definition Process

If you are not sure which application would be most effective for defining your organization's cybersecurity roles, you can follow these steps to determine which to choose:

1. **Compare the roles used by your organization to the streamlined roles.** Distribute the roles to your organization's Subject Matter Experts (SMEs). Ask them to compare organizational roles against the streamlined applications.
2. **Select a streamlined or customized approach.** Some organizations may adopt the streamlined roles; others may have segmented roles with a 1-to-1 relationship with specialty areas (and may need to develop customized roles).
3. **Validate the applicable tasks.** In the example of Computer Network Defense Specialist, review the task lists for Computer Network Defense and Computer Network Defense Infrastructure Support.
4. **Apply the Framework components to other human capital activities.** If these tasks are applicable to an organization's roles, the Framework competency and KSA inventories may be used in human capital activities.



Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

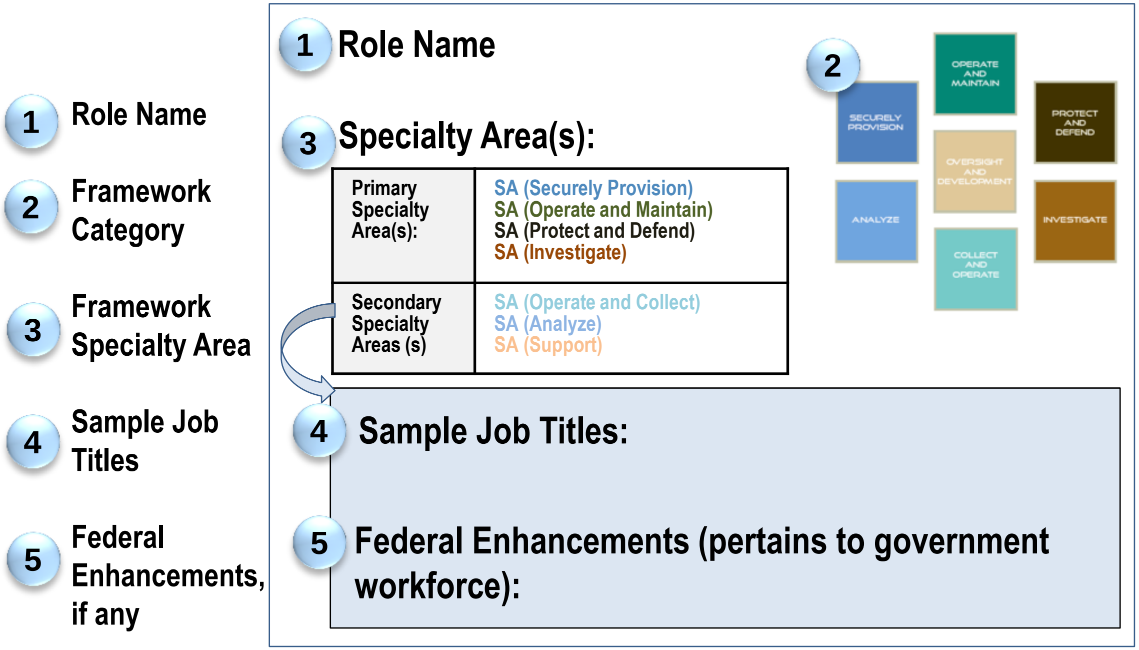
Contact Us

Streamlined Roles (Example)

If your organization has a limited number or type of cybersecurity positions, you may prefer to choose the streamlined roles. Fed CIOC developed 13 Framework-based streamlined cybersecurity roles to promote consistency and standardization of the cybersecurity workforce.

Each role consists of sample job titles and definition, the related Framework category, the Framework specialty areas, and any enhancements that pertain specifically to the Federal workforce.

This graphic depicts a template of a streamlined cybersecurity role.



1 Role Name

2 Framework Category

3 Framework Specialty Area

4 Sample Job Titles

5 Federal Enhancements, if any

1 Role Name

3 Specialty Area(s):

Primary Specialty Area(s):	SA (Securely Provision) SA (Operate and Maintain) SA (Protect and Defend) SA (Investigate)
Secondary Specialty Areas (s)	SA (Operate and Collect) SA (Analyze) SA (Support)

4 Sample Job Titles:

5 Federal Enhancements (pertains to government workforce):

The 13 streamlined cyber roles identified by Fed CIOC are below. Click on a role to see sample titles, a definition, and Framework category and specialty areas.

- Systems Operations Professional
- Data Administrator
- Computer Network Defense (CND) Specialist
- Digital Forensics and Incident Response Analyst
- Information Security Auditor
- Information Systems Security Officer
- Information Systems Security Manager
- Information Security Architect
- Risk and Vulnerability Analyst
- Software Developer
- Information Systems Security Engineer
- Strategic Planning and Policy Development Professional
- Chief Information Security Officer (CISO)

Click HERE for the process of adopting the Fed CIOC roles.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

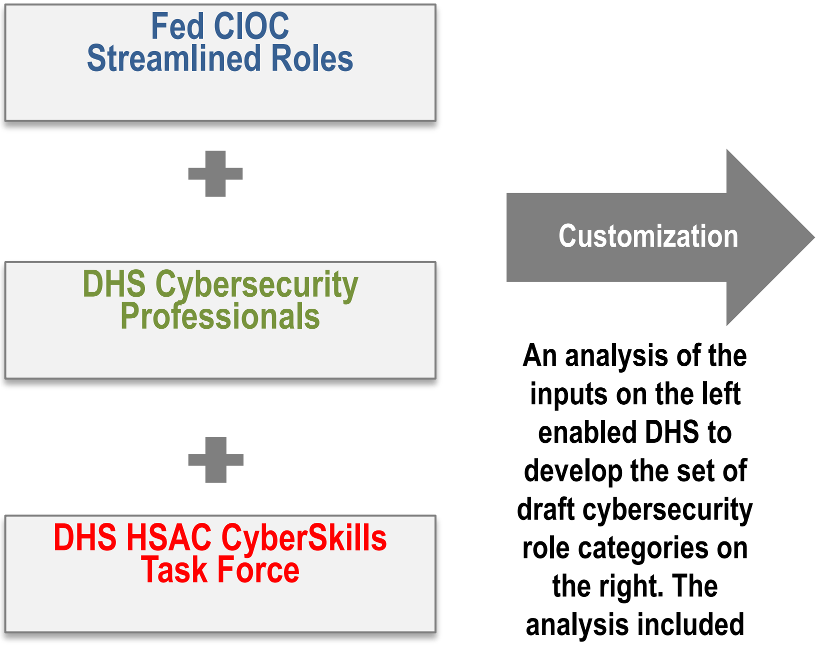
Contact Us

Customized Roles (Preliminary Example)

If your organization has many unique or specialized positions, you may choose to develop customized cybersecurity roles. This application has been demonstrated by DHS's Cyber Workforce Initiative (CWI).

An extensive review of DHS's workforce revealed many initial unique cybersecurity roles across the organization. DHS employed a process to establish generalized cybersecurity draft role categories linked to Fed CIOC Streamlined Roles, Framework Specialty Areas, Critical Skills, and the DHS Workforce.

DHS analyzed 3 things:


Fed CIOC Streamlined Roles
DHS Cybersecurity Professionals
DHS HSAC CyberSkills Task Force
Customization

An analysis of the inputs on the left enabled DHS to develop the set of draft cybersecurity role categories on the right. The analysis included interviewing and other qualitative analysis activities.

23 ROLE CATEGORIES:

- Chief Information Security Officer (CISO)/Chief Information Officer (CIO)
- Computer Network Defense (CND) Specialist
- Cyber Intelligence Operations & Analysis Professional
- Cyber Program/ Project Manager
- Cybersecurity Training, Outreach & Awareness Professional
- Cyber Workforce Planner
- Database Administrator (DBA)
- Forensic Examiner/Digital Media Analyst
- Incident Management & Incident Response (IMIR) Professional
- Information Security and Enterprise/ Systems Architect
- Information Security (INFOSEC) Auditor
- Information Systems Security Engineer (ISSE)
- Information Systems Security Manager (ISSM)
- Information Systems Security Officer (ISSO)
- Knowledge Officer
- Network Administrator
- Penetration Tester
- Risk & Vulnerability Specialist
- Secure Software Developer / Code Reviewer
- Standards and Research & Development Professional
- Strategic Planning & Policy Professional
- Systems Administrator
- Technical Customer Support

Role Category Color LEGEND

RED - align to the 10 mission critical job tasks identified by the HSAC CyberSkills task Force.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Customized Roles (Preliminary Example)

This is an example of one of DHS's customized roles.

Penetration Tester

Aligned DHS Roles to-date	**Vulnerability Assessment Programs (Blue Team)** **Penetration Tester (Red Team)** **Exploit Engineer/Developer**	
Prominent Specialty Areas: & Critical Task	• Systems Security Architecture • Security Engineering • Architecting for Building Security In • Information Assurance (IA) Compliance • Exploitation Analysis	• Application Penetration Tester • Vulnerability Assessment and Management • Systems Security Analysis • System and Network Penetration Tester • Penetration Testing

Role Definition: Follows a systematic methodology to assess, identify and demonstrate attack vectors and their impacts to provide risk mitigation/remediation strategies. Maintains knowledge of system architecture designs, current threats and methodologies (TTPs) and security requirements (e.g., NIST, FISMA, etc.) to conduct sophisticated penetration testing throughout the lifecycle. Demonstrates capability in running advanced exploitation techniques without the use of automated tools.

***Source Definition:** Focus Group SMEs for System/Network/Application Penetration Testing

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

STEP 2: Competency Modeling

Competency Model Links

Overview What is a Competency? Steps to Development Competency Model Components Template

A second step recommended for adopting the Framework is for organizations to develop role-specific, competency models for cybersecurity workers.

Competency models will allow an organization to:

- ✓ Establish a baseline of role-specific cybersecurity competencies to determine capability requirements for respective cybersecurity roles and provide parameters for building an effective, mission-focused cybersecurity workforce; thereby reducing organizational risk.
- ✓ Assess skills and identify gaps and promote cybersecurity innovation by identifying training needs of a high-performing, diverse workforce.
- ✓ Build cybersecurity competency across the organization and create a more comprehensive and structured approach to employee development.
- ✓ Inform workforce planning and talent management efforts supporting organization missions.
- ✓ Consider small-scale or transformational changes that may require just-in-time role-specific training.

DHS is applying the Framework by developing role-specific, cybersecurity competency models. This initiative is led by DHS's Cybersecurity Workforce Initiative (CWI).

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

What is a Competency? A Competency Model?

Competency Model Links

Overview What is a Competency? Steps to Development Competency Model Components Template

Competencies are individual or organizational attributes that are required for successful performance. Competencies in our application will describe workforce characteristics comprised of behaviors individuals must exhibit to successfully perform their specific role. These are considered technical competencies which are unique to a specific role and distinguish it from others. Technical competencies are most useful for identifying capabilities in mission critical occupational series and functional areas (like the cybersecurity workforce). They provide a common language that facilitates standard integration into HC initiatives.

A **competency model** comprises of:

- Competency titles and definitions
- May include behavioral indicators (BIs) describe to what degree/proficiency an individual possesses a competency and how the competencies manifest themselves in on-the-job behaviors. Typically they increase in scope, complexity, responsibility at the higher levels of proficiency
- Subject Matter Expert Importance Ratings
- Subject Matter Expert Criticality Ratings

In the case of the cybersecurity competency models developed by DHS CWI, the Framework specialty areas and specialty area definitions were leveraged to develop the competencies and competency definitions within the model. A unique technical competency list was customized for each DHS role competency model. The technical competencies identified may be specific to a particular role or shared across similar models (i.e. network administrators and system administrators may share similar competencies, but their behavioral indicators or required proficiency targets may vary based on distinct job requirements).

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Steps to Developing Custom Competency Models

Competency Model Links

Overview What is a Competency? Steps to Development Competency Model Components Template

This table provides a high-level overview of an approach to a cybersecurity technical competency model development process.

The steps can be followed exactly, or can be customized depending on your organizational environment.

Step	Activity
1	Identify organization leadership points of contact (POCs). These are senior level managers that understand their organization's cybersecurity workforce.
2	Identify a particular cybersecurity role(s) within the organization that is considered mission critical and identify the specialty areas/competencies that are aligned to the role within that area or sub-organization.
3	Ask POCs to identify SMEs with roles similar to the cybersecurity role(s) previously identified.
4	Conduct focus groups with the cybersecurity SMEs to validate the role-specific, specialty areas/competencies that have been aligned to their role and to develop and refine unique BIs that represent observable behaviors for demonstrating each proficiency level.
5	Finalize the role's competency model based on SME input. See a template.
6	Validate the final competency model with the SMEs by having them determine importance and criticality ratings.
7	Validate the final competency model with the organization's leadership POCs.
8	Finalize the competency model and implement.

Components of a Competency Model

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Competency Model Links

Overview What is a Competency? Steps to Development Competency Model Components Template

The final cybersecurity competency models will consist of the following:

- **Custom Cybersecurity Role Definition** to describe the type of work and the context of the role.
- **Specialty Areas** (either streamlined by using the Framework or Customized for your organization) required for successful job performance in the role with a definition.
- **Unique Role-Specific BIs** for demonstrating varying degrees of proficiency in each specialty area (i.e., competency). BIs are examples of actions or activities that describe how competencies manifest as observable, on the job behaviors.
- **Criticality Rankings** for each specialty area in terms of its importance for successful job performance in the role.
- **Required Upon Entry Rankings** for each specialty area in terms of whether it is required upon entry into a role or can be developed/trained on the job.
- **Proficiency Targets** identified for each career level as they pertain to each specialty area within a role (i.e., the degree in which an individual would be expected to be proficient in a particular specialty area based on their career level within the role).

Competency Model Template

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Competency Model Links

Overview What is a Competency? Steps to Development Competency Model Components Template

This is an illustration of the components of a competency model.

Enter Specialty Area Title Here	Enter Specialty Area Definition Here	
Example Tasks Identified as Part of Competency: • List Examples of Key Tasks Here		
BEHAVIORAL INDICATORS		
0 No Proficiency	• Enter Behavioral Indicators Here	
1 Basic	• Enter Behavioral Indicators Here	
2 Intermediate	• Enter Behavioral Indicators Here	
3 Advanced	• Enter Behavioral Indicators Here	
4 Expert	• Enter Behavioral Indicators Here	
CRITICALITY		
Importance	Required at Entry	Criticality
ENTER IMPORTANCE RATING HERE	ENTER REQUIRED AT ENTRY RATING HERE	ENTER CRITICALITY RATING HERE
PROFICIENCY TARGETS		
(ENTER GS RANGE)	(ENTER GS RANGE)	(ENTER GS RANGE)
Enter Proficiency Target (ex. 2 – Intermediate)	Enter Proficiency Target	Enter Proficiency Target

[Contents](#)

[What is the Framework?](#)

[Categories](#)

[Specialty Areas](#)

[Benefits](#)

[HCM Impact](#)

[Adoption](#)

[STEP 1: Role Definition](#)

- [Streamlined Roles](#)
- [Customized Roles](#)

[STEP 2: Model Competencies](#)

[STEP 3: Plan Your Workforce](#)

[STEP 4: Plan for the Future](#)

[Contact Us](#)

STEP 3: Workforce Planning Overview

Workforce Planning Links

[Overview](#) [What is Workforce Planning?](#) [Steps to Process](#) [White Papers](#)

As the demands of global business, computing, and society revolve around information technology, cybersecurity workload is increasing faster than cybersecurity professionals can meet the demand. As such, an emerging priority in cybersecurity is the question of how organizations track, assess, grow, and shape this specialized workforce.

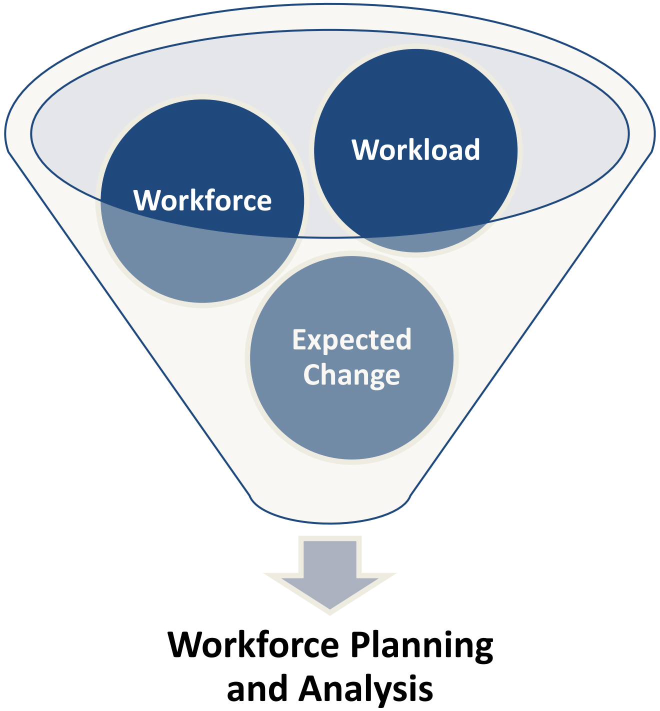
Workforce planning is the process organizations can use to address these concerns. Workforce Planning analyzes demand issues and helps organizations close the workforce gap in a systematic way.

Workforce Planning helps answer:

- What does our current workforce look like?
- How many cybersecurity workers do we have?
- What positions do these individuals hold?
- What is their current workload?

Workforce Planning informs decisions organizations make to correctly plan for the future:

- Do we anticipate changes in workload?
- Are our workers correctly aligned to the work?
- What competencies should the position require based on the workload?
- Is additional training needed if the work is changing? Are new positions needed?
- Do we have the budget to fund the positions needed to meet our goals and objectives?



Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

What is Workforce Planning?

Workforce Planning Links

Overview What is Workforce Planning? Steps to Process White Papers

Workforce planning is a systematic way for organizations to determine future human capital requirements (demand), identify current human capital capabilities (supply), and design and implement strategies to transition the current workforce to the desired future workforce. Good workforce planning is designed in a repeatable and reliable fashion, highlighting risks and forecasting needs over time.

Effective workforce planning highlights potential risk areas associated with aligning workforce to work. Applied correctly, workforce planning allows organizations to adjust resources to meet future workloads, patterns of work, and fundamental changes in how work is accomplished. A workforce planning approach must fit the needs of a specific organization and account for unique characteristics of the cybersecurity profession.

Leading practice workforce planning consists of three components:

- **Process:** Establishing an integrated and consistent means of diagnosing workforce needs and risks. This includes a defined model, data and analytics.
- **Strategy:** Providing a direct line of sight between business and workforce requirements. This includes a shared vision, governance, and continuous monitoring or performance.
- **Infrastructure:** Supporting execution of an effective and repeatable workforce planning process. This includes a healthy workforce or people, collaboration across levels and enabling technology.

A **workforce planning process,** as described on the following page, identifies and quantifies the workload and workforce requirements unique to an organization; and analyzes the skills needed to fill the gap in workforce.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

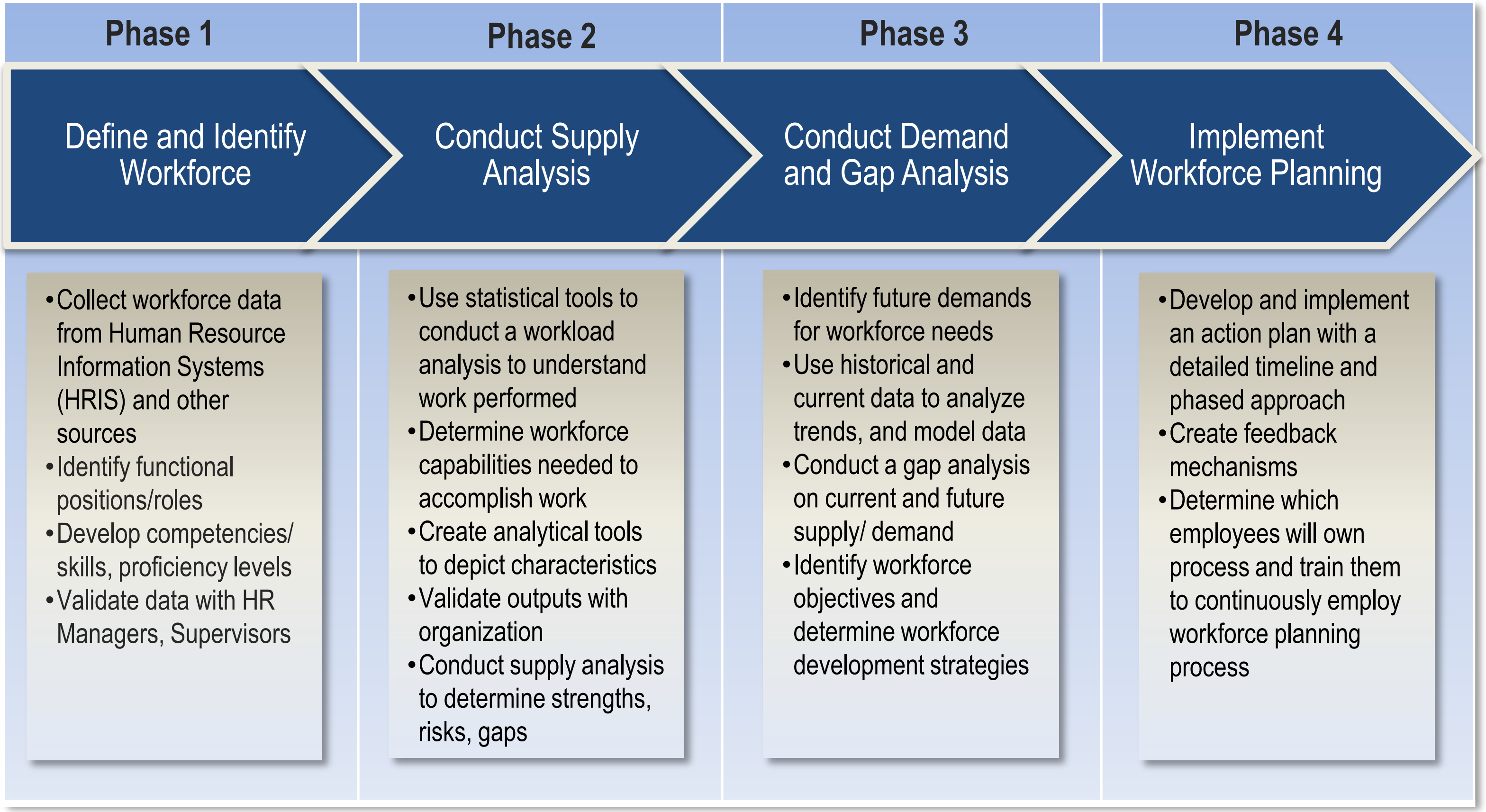
Contact Us

Workforce Planning Process

Workforce Planning Links

Overview What is Workforce Planning? Steps to Process White Papers

Using a Workforce Planning Process, such as the example provided below, an organization can conduct a cybersecurity workforce and workload analysis, enabling it to identify current and future needs and potential gaps which may impact an organization's ability to meet goals and objectives.



Phase 1

Define and Identify Workforce

- Collect workforce data from Human Resource Information Systems (HRIS) and other sources
- Identify functional positions/roles
- Develop competencies/ skills, proficiency levels
- Validate data with HR Managers, Supervisors

Phase 2

Conduct Supply Analysis

- Use statistical tools to conduct a workload analysis to understand work performed
- Determine workforce capabilities needed to accomplish work
- Create analytical tools to depict characteristics
- Validate outputs with organization
- Conduct supply analysis to determine strengths, risks, gaps

Phase 3

Conduct Demand and Gap Analysis

- Identify future demands for workforce needs
- Use historical and current data to analyze trends, and model data
- Conduct a gap analysis on current and future supply/ demand
- Identify workforce objectives and determine workforce development strategies

Phase 4

Implement Workforce Planning

- Develop and implement an action plan with a detailed timeline and phased approach
- Create feedback mechanisms
- Determine which employees will own process and train them to continuously employ workforce planning process

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Workforce Planning White Papers

Workforce Planning Links

Overview What is Workforce Planning? Steps to Process White Papers

NICE developed two White Papers addressing the need of Workforce Planning within the cybersecurity field and to make recommendations on how to conduct workforce planning within this field.

Both papers are available now by contacting the DHS Cybersecurity Education Office (CEO). They will also be posted on the National Institute for Cybersecurity Studies (NICCS) Portal when it is launched.

Best Practices for Cybersecurity Workforce Planning White Paper

This paper introduces workforce planning methodologies for cybersecurity, and guidance for organizations. It synthesizes best practices from over 70 Federal organizations, interviews, workforce planning benchmarking studies, Federal reports, and workforce planning guides, and organized across three best practice components — process, strategy, and infrastructure.

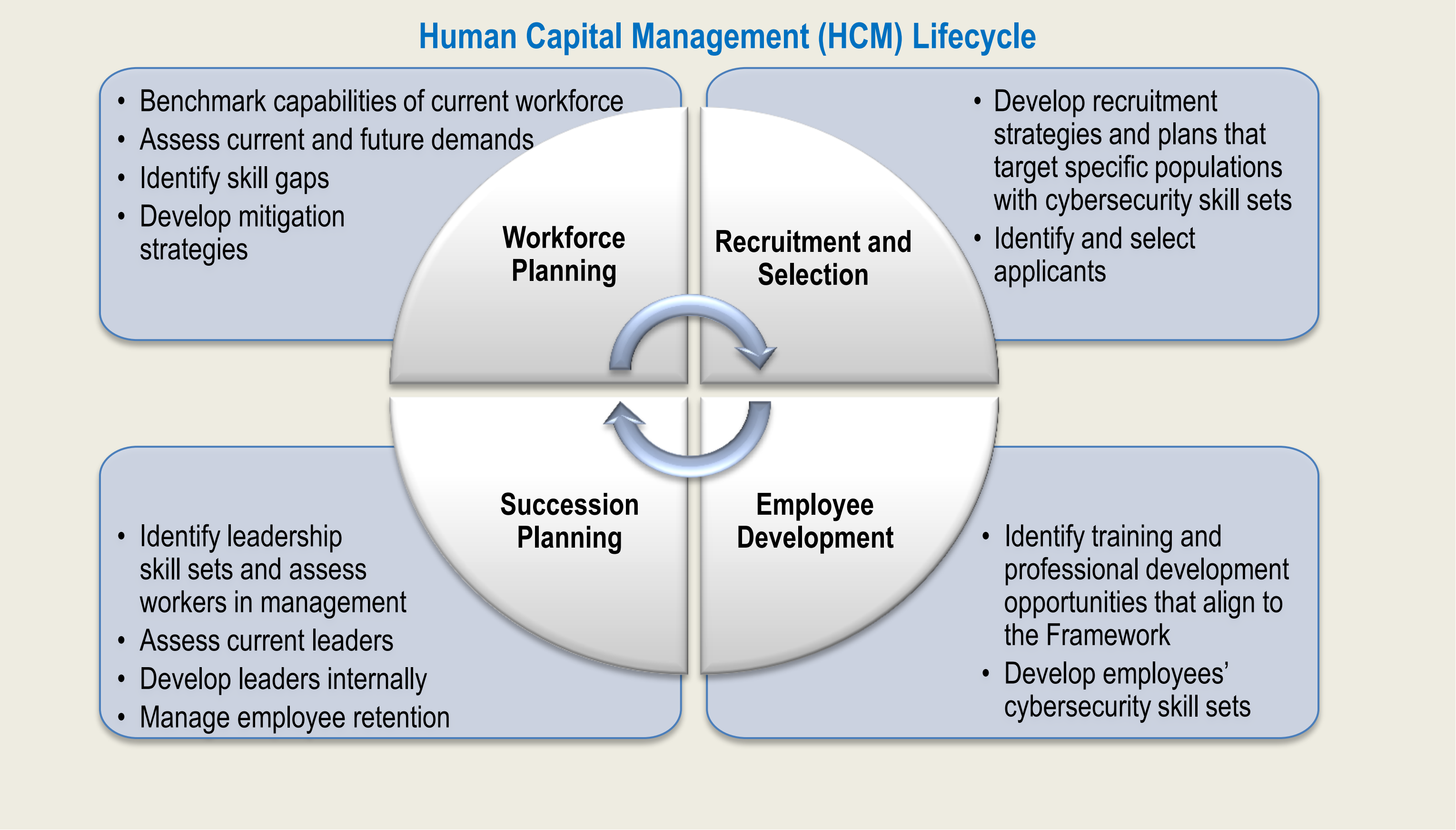
Cybersecurity Capability Maturity Model (CMM) White Paper

This paper introduces a qualitative management tool, a Cybersecurity Workforce Planning CMM, to help organizations apply the elements of best practice workforce planning to analyze their cybersecurity workforce requirements and needs. The CMM provides a structure for organizations to baseline current capabilities in cybersecurity workforce planning, and enables leaders to make better decisions about how to support progression and what investments to make in regard to cybersecurity human capital initiatives.

STEP 4: Plan for the Future

Once you have defined your organization's roles, developed competency models, and conducted workforce planning, you are ready to continue planning for the future.

When launched, more information will be available on the **National Institute for Cybersecurity Studies (NICCS)** web portal to help you link additional Human Capital efforts to the National Cybersecurity Workforce Framework.



Human Capital Management (HCM) Lifecycle

Workforce Planning

- Benchmark capabilities of current workforce
- Assess current and future demands
- Identify skill gaps
- Develop mitigation strategies

Recruitment and Selection

- Develop recruitment strategies and plans that target specific populations with cybersecurity skill sets
- Identify and select applicants

Succession Planning

- Identify leadership skill sets and assess workers in management
- Assess current leaders
- Develop leaders internally
- Manage employee retention

Employee Development

- Identify training and professional development opportunities that align to the Framework
- Develop employees' cybersecurity skill sets

Contact Us

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

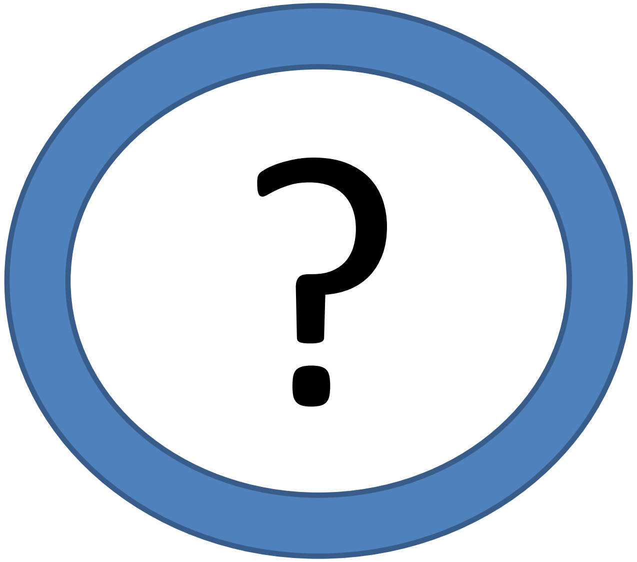
STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

For additional information on the Framework, and for any questions, please visit:

http://www.nist.gov/nice/framework/



Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

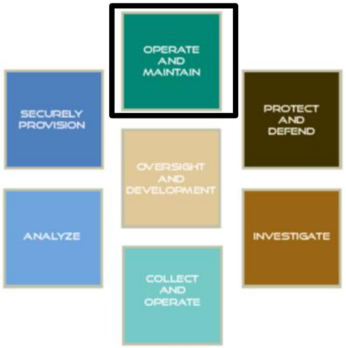
STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Systems Operations Professional

SYSTEMS OPERATIONS PROFESSIONAL



Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	System Administration (Operate and Maintain) Network Services (Operate and Maintain)
Secondary Specialty Area(s):	*N/A*

Systems Operations Professional: Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, account creation and administration. Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

Federal Enhancements:

- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*
- *This role maps to the Systems Operations and Maintenance Professional Workforce Development Matrix published in December 2011 in the "Cybersecurity Workforce Development Matrix Resource Guide." (www.cio.gov – Workforce - Document Library)*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

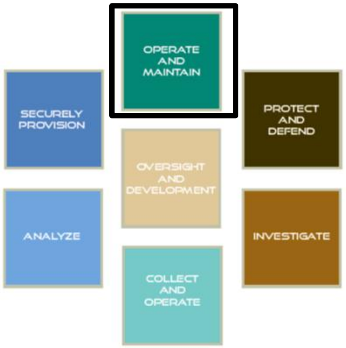
STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Data Administrator

DATA ADMINISTRATOR



Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Data Administration (Operate and Maintain)
Secondary Specialty Area(s):	Knowledge Management (Operate and Maintain)

Data Administrator: Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

Federal Enhancements:

- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Computer Network Defense Specialist

Computer Network Defense Specialist

OPERATE AND MAINTAIN
SECURELY PROVISION
PROTECT AND DEFEND
OVERSIGHT AND DEVELOPMENT
ANALYZE
INVESTIGATE
COLLECT AND OPERATE

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Computer Network Defense (CND) Analysis (Protect and Defend) Computer Network Defense (CND) Infrastructure Support (Protect and Defend)
Secondary Specialty Area(s):	*N/A*

Computer Network Defense Specialist: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats. Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.

Federal Enhancements:

- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

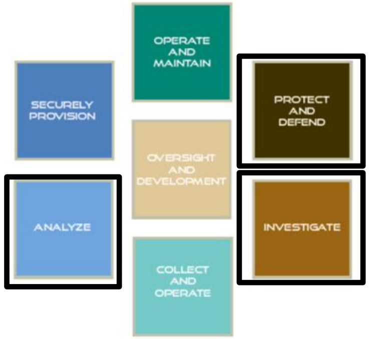
STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Digital Forensics & Incident Response Analyst

DIGITAL FORENSICS & INCIDENT RESPONSE ANALYST



Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Incident Response (Protect and Defend) Digital Forensics (Investigate)
Secondary Specialty Area(s):	Threat Analysis (Analyze)*

Digital Forensics and Incident Response Analyst: Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities. Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.

Federal Enhancements:

- The Analyst is responsible for disseminating and reporting cyber-related activities, conducing vulnerability analyses and risk management of computer systems and all applications during all phases of the systems development lifecycle
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

* *If adding the Secondary Specialty Area, this role may be considered unique and highly specialized.*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

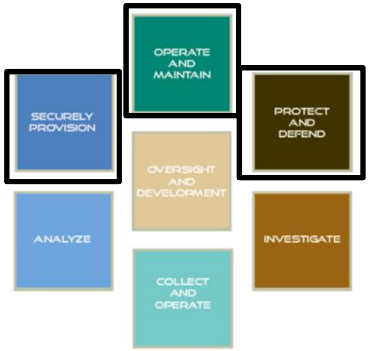
Contact Us

Information Security Auditor

INFORMATION SECURITY AUDITOR

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Information Assurance (IA) Compliance (Securely Provision) Vulnerability Assessment and Management (Protect and Defend)
Secondary Specialty Area(s):	Test and Evaluation (Securely Provision) Systems Security Analysis (Operate and Maintain)



Information Security Auditor: Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new information technology (IT) systems meet the organization's information assurance (IA) and security requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives. Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

Federal Enhancements:

- The Information Security Auditor is so named to address the reality that these combined specialties may be performed outside of the CIO organization (i.e., Inspector General)
- When performed from an internal perspective, this application may be alternatively know as an Assessor
- The Information Security Auditor relates to the Security Control Assessor defined by NIST SP 800-37. To this end, the IS Auditor is meant to audit the management, operational, and technical security controls of an information system to determine their effectiveness
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Information Security Architect

Information Security Architect

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Systems Security Architecture (Securely Provision) Systems Development (Securely Provision)
Secondary Specialty Area(s):	Information Assurance (IA) Compliance (Securely Provision)

OPERATE AND MAINTAIN
SECURELY PROVISION
PROTECT AND DEFEND
OVERSIGHT AND DEVELOPMENT
ANALYZE
INVESTIGATE
COLLECT AND OPERATE

Information Security Architect: Develops system concepts and works on the capabilities phases of the system development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes. Works on the development phases of the systems development lifecycle.

Federal Enhancements:

- The Information Security Architect develops security design requirements through sound design methodology, adequate security control application, and effective configuration practices
- The Information Security Architect ensures secure architectural solutions are incorporated into every aspect of the enterprise architecture supporting an organization’s key business processes and organizational mission
- The Information Security Architect provides the interface between the Enterprise Architect and the Information System Security Engineering as detailed in NIST SP 800-37
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Information Systems Security Engineer

Information Systems Security Engineer

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Systems Security Architecture (Securely Provision) Systems Development (Securely Provision)
Secondary Specialty Area(s):	Test and Evaluation (Securely Provision) Systems Requirements Planning (Securely Provision)

OPERATE AND MAINTAIN
SECURELY PROVISION
PROTECT AND DEFEND
OVERSIGHT AND DEVELOPMENT
ANALYZE
INVESTIGATE
COLLECT AND OPERATE

Information Systems Security Engineer: Develops system concepts and works on the capabilities phases of the system development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes. Works on the development phases of the systems development lifecycle.

Federal Enhancements:

- The Engineer ensures that security requirements and security engineering practices are incorporated throughout the system development life cycle and engineering maintenance of solutions, applications, products, information systems and network environments to minimize risk to the organization
- Best practices regularly employed by the Information Systems Security Engineer include ensuring adherence to the agency’s enterprise architecture, software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques*
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

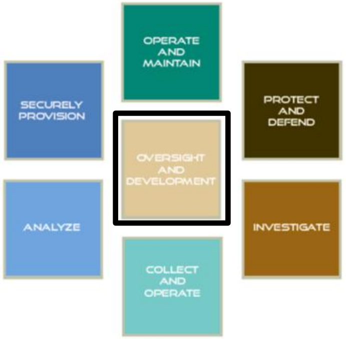
STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Information Systems Security Manager

INFORMATION SYSTEMS SECURITY MANAGER (ISSM)*



Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Information Systems Security Officer (Oversight and Development)
Secondary Specialty Area(s):	*N/A*

Information Systems Security Manager: Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

Federal Enhancements:

- The ISSM is responsible for the information assurance of a program, organization or enclave
- The ISSM serves as an advocate for all disciplines within the security program including the development and subsequent enforcement of the organization’s security awareness programs, business continuity and disaster recovery plans, and all industry and governmental compliance issues
- The ISSM works closely with and in some cases may oversee the ISSO
- In large organizations, the ISSM may be superseded by or report to an IS Program Manager
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

* *See Information Systems Security Officer (ISSO) – these roles vary in organizations – carefully note Federal Enhancements to explain differences.*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

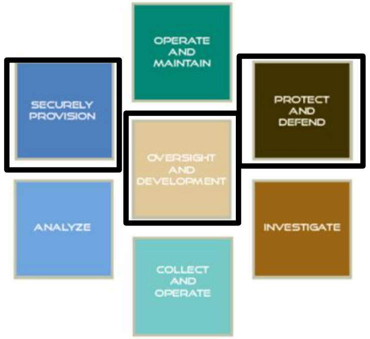
Contact Us

Information Systems Security Officer

INFORMATION SYSTEMS SECURITY OFFICER (ISSO)*

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Information Systems Security Officer (Oversight and Development)
Secondary Specialty Area(s):	Information Assurance Compliance (Securely Provision) Vulnerability Assessment and Management (Protect and Defend)



Information Systems Security Officer: Oversees the information assurance (IA) program of an information system in or outside the network environment; may include procurement duties.

Federal Enhancements:

- The ISSO communicates with the business at the system level and understands security threats and vulnerabilities to the operations and the system's environment
- The ISSO ensures that the appropriate operational posture is maintained for an information system and is responsible for advising system owners and interfacing with users
- The ISSO will have the technical expertise necessary to oversee the day-to-day security operations of a system and may direct others who manage those operations (e.g., system administrators, database administrators and developers)
- In organizations where the ISSO role is performed by non-government employees, the strategic system decisions are made by the ISSM or CISO
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

** See Information Systems Security Manager (ISSM) – these roles vary in organizations – carefully note Federal Enhancements to explain differences.*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Risk and Vulnerability Analyst

Risk and Vulnerability Analyst

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Vulnerability Assessment and Management (Protect and Defend) Systems Security Analysis (Operate and Maintain)
Secondary Specialty Area(s):	*N/A*

OPERATE AND MAINTAIN
SECURELY PROVISION
PROTECT AND DEFEND
OVERSIGHT AND DEVELOPMENT
ANALYZE
INVESTIGATE
COLLECT AND OPERATE

Risk and Vulnerability Analyst: Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations. Conducts the integration/testing, operations, and maintenance of systems security.

Federal Enhancements:

- This Risk and Vulnerability Analyst adheres to relevant compliance regulations and responds to risk management policies and procedures
- The Risk and Vulnerability Analyst is seen as a key participant in the risk management process as defined by NIST SP 800-37
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

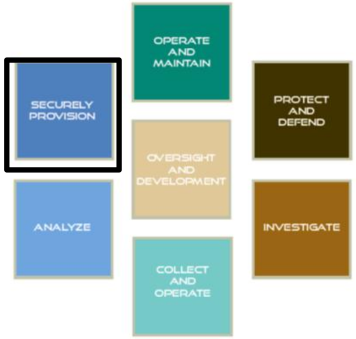
STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Software Developer

SOFTWARE DEVELOPER



Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Software Assurance and Security Engineering (Securely Provision)
Secondary Specialty Area(s):	*N/A*

Software Developer: Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

Federal Enhancements:

- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*
- *This role maps to the Information Security Systems and Software Development Professional Workforce Development Matrix published in December 2011 in the "Cybersecurity Workforce Development Matrix Resource Guide." (www.cio.gov – Workforce - Document Library)*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

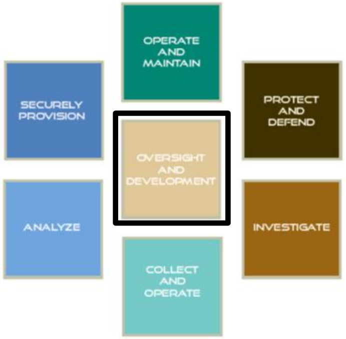
Contact Us

Strategic Planning & Policy Development Professional

Strategic Planning & Policy Development Professional

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Strategic Planning and Policy Development (Oversight & Development)
Secondary Specialty Area(s):	Legal Advice and Advocacy (Oversight & Development)



Strategic Planning and Policy Development Professional: Applies knowledge of priorities to define an entity's direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest. Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.

Federal Enhancements:

- The Strategic Planning & Policy Development Professional also applies knowledge of relevant laws, regulations, guidance and standards to facilitate sound policy development by the organization
- The Strategic Planning & Policy Development Professional develops policy in accordance with internal/organizational requirements as well as external security requirements (e.g., FISMA)
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*

Click HERE to return to the Role Definition section.

Contents

What is the Framework?

Categories

Specialty Areas

Benefits

HCM Impact

Adoption

STEP 1: Role Definition

- Streamlined Roles
- Customized Roles

STEP 2: Model Competencies

STEP 3: Plan Your Workforce

STEP 4: Plan for the Future

Contact Us

Chief Information Security Officer (CISO)

CHIEF INFORMATION SECURITY OFFICER (CISO)

Foundational NIST NICE Specialty Area(s):

Primary Specialty Area(s):	Security Program Management (Chief Information Security Officer (CISO)) (Oversight & Development)
Secondary Specialty Area(s):	*N/A*

OPERATE AND MAINTAIN
SECURELY PROVISION
PROTECT AND DEFEND
OVERSIGHT AND DEVELOPMENT
ANALYZE
INVESTIGATE
COLLECT AND OPERATE

Chief Information Security Officer (CISO): Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.

Federal Enhancements:

- The CISO leads the evaluation and assessment of the security program to ensure that all aspects are in compliance with security requirements (e.g., FISMA), while understanding security threats and vulnerabilities to operations and the organization's environment
- In limited cases and in small agencies, the CISO may also assess the management, operational, and technical security controls of the information system to ensure effectiveness
- The CISO is an acknowledged role title at the agency level but the above responsibilities may be fully performed under a different title at the program, sub-agency or component level
- The CISO's authority to carry out the above functions is delegated from the CIO, in accordance with Clinger-Cohen/FISMA requirements
- *Additional enhancements will be established based on Matrix Project SME feedback and CIO Council direction (as applicable)*
- *This role maps to the Systems Operations and Maintenance Professional Workforce Development Matrix published in December 2011 in the "Cybersecurity Workforce Development Matrix Resource Guide." (www.cio.gov – Workforce - Document Library)*

Click HERE to return to the Role Definition section.